Risk in Review
Re-evaluating how your company addresses risk

Market shifts and reactive business transformations may be combining to open critical capability gaps in risk management.

March 2014

pwc

Table of contents

The heart of the matter

New risks, new opportunities

Throughout 2013, public- and private-sector organizations coped with intense market shifts and new challenges. The Eurozone finally emerged from recession, but GDP growth in the US slowed to 1.9% from 2.8% in 2012, and growth among the BRICs cooled. The collapse of the Rana Plaza garment factory in Bangladesh made conditions for workers in developing countries a major public issue. Sweeping new laws such as the Affordable Care Act (ACA) took effect in the US, while contractor Edward Snowden's massive leak of classified National Security Agency documents brought third-party risks to the fore.

Against this backdrop, PwC conducted its fourth annual risk survey in the fall of 2013, polling 1,940 executives across 37 countries to seek a detailed picture of the state of risk in today's business climate. Respondents brought perspectives from five broad organizational sectors: financial services; healthcare; consumer and industrial products and services (CIPS); technology, information, communications, and entertainment (TICE); and government agencies. This study presents key findings and insights from that survey, as well as from a series of related, in-depth executive interviews.

Over the next 18 months, executives in our survey expect ongoing market changes will affect their firms in three key areas: technological change and related IT risks, increasing regulatory complexity, and rapidly changing customer needs. To address these shifts, companies continue to undergo dramatic transformation, changing their strategies and driving radical internal change: Three out of four survey respondents say their firm has recently undergone a transformation initiative, is doing so, or will in the near future.

The combination of market shifts and the business changes undertaken in response is intensifying risk overall, with 75% of executives reporting that risks to their businesses are increasing. Even more worrying, our research finds that these shifts are opening capability gaps in risk management, particularly around data management, business strategy, and technology. Alden Toevs, Group CRO at Commonwealth Bank of Australia, defines the challenge: "New technologies, faster rate of change, and significant increases in regulatory scrutiny and accountability mean the risk management function must evolve by being more agile, and at the same time balance risk, return, and growth."

To close these capability gaps, executives are focusing on creating a risk-aware culture, developing processes to continuously identify and monitor risks, and conducting more non-financial audits. Companies expect to make significant progress toward greater risk maturity in four areas:

- Aligning business and risk strategy
- Adopting and applying risk appetite statements
- Managing stakeholder expectations
- Improving risk monitoring and reporting

"New technologies, faster rate of change, and significant increases in regulatory scrutiny and accountability mean the risk management function must evolve by being more agile, and at the same time balance risk, return, and growth."

—Alden Toevs, Group CRO, Commonwealth Bank of Australia

Executives are confident about their progress: Most believe their organizations manage risk well, and express greater satisfaction with their level of risk management competency than they did in last year's survey. But even risk-mature firms (risk leaders) are moving aggressively toward higher levels of competency, with more than four out of five growing their expertise across a broader range of risk processes and skills — for example, developing the capability to identify and track risks across the organization, conducting more non-financial audits, and devoting more attention to monitoring emerging risks. Perhaps as a result, risk leaders are less likely to report capability gaps and are far more likely to be satisfied with their overall resilience.

Looking to the future, our analysis reveals the following key imperatives for survey respondents at three levels of risk management maturity:

- **Early-stage organizations.** These companies must put the basic elements of risk management in place, de-siloing risk processes by extending them across the organization.
- **Developing organizations.** These organizations must link business and risk strategy, consolidate risk reporting, and build an organization-wide risk culture.
- **Risk leaders.** Companies with the most mature risk management systems must put in place regular review, evaluation, and updating of their processes, incentives, and risk culture.

PwC conducted its fourth annual risk survey in the fall of 2013, polling ***1,940*** *executives across* ***37*** *countries to seek a detailed picture of the state of risk in today's business climate. This study presents key findings and insights from that survey, as well as from a series of related, in-depth executive interviews.*

Survey and interview methodology

In fall 2013, PwC surveyed 1,940 executives across 37 countries. The sample included a range of sectors, with consumer and industrial products and services (CIPS) representing more than one third of respondents and financial services more than one fourth. Respondents represented various facets of the organization, including internal audit (73% of respondents), management and the board (10%), the finance function (10%), risk and compliance (6%), and other (1%). Roughly two thirds of respondents were from organizations with annual revenues of $1 billion and above. A large majority (81%) represented companies headquartered in industrialized regions, with slightly more than half of those based in North America.

To supplement the survey findings, we conducted in-depth interviews with risk management executives at the following leading organizations:

- **Anglo American:** Mark Newlands, Head of Risk Management and Business Assurance
- **AutoNation:** Dennis Royer, Senior Director of Risk Management
- **C. R. Bard:** Pat Roche, Vice President, Information Technology Solutions
- **Commonwealth Bank of Australia:** Alden Toevs, Group CRO
- **Eastman Chemical Company:** Peter Roueche, Director, Enterprise Risk and Insurance
- **Google:** Lisa Lee, Chief Audit Executive
- **Microsoft:** Melvin Flowers, Corporate Vice President of Internal Audit
- **Swiss Re:** David Cole, Dutch and American Group CRO

Identifying risk leaders

To understand what differentiates leaders in risk management, we segmented respondents based on the question, "Which stage of maturity best describes your risk management framework?" Each organization rated itself on a scale of 1 to 5 across six areas of practice: risk management strategy, risk appetite, stakeholder management, risk monitoring and reporting, risk culture, and risk-adjusted performance incentives. Three groups emerged:

- **Risk leaders** scored 23 or higher; 237 organizations qualified.
- **Developing organizations** scored between 14 and 22; 688 organizations qualified.
- **Early-stage organizations** scored below 14; 498 organizations qualified.

Financial services represented nearly half of risk leaders, and CIPS accounted for more than a quarter. However, by respondent title, organization size, and geographic location of headquarters, the breakdown of risk leaders was similar to the overall sample.

An in-depth discussion

Sweeping market and business change translates to increasing risk

Risks are rising across the board, a trend acknowledged by three out of four respondents to our survey (75%), only slightly less than last year (81%). For the next 18 months, a majority of executives foresee continued and significant changes in the world marketplace that will dramatically impact their companies. Healthcare organizations, facing a radically changing market framework in the US, are especially concerned (86%). While macro risks associated with the Eurozone crisis appear to have moderated somewhat, "the interconnectedness of risks and pace of change continue to increase," says Brian Brown, PwC US Risk Assurance Innovation Center Leader.

While headlines focus on sluggish economic recovery and moves toward fiscal austerity in many parts of the world, top executives' attention has shifted: In all, only 42% of respondents rank global economic shifts and uncertainty as major drivers of change over the next 18 months. This stands in sharp contrast to last year, when the top-ranked risk overall was increased recessionary pressures (72%). Instead, respondents expect the most impactful forces over the next 18 months to be technological change and IT risks (58%) (see Figure 1).

"Many new, high-impact risks are around global expansion and cyber-attacks," says Alden Toevs of Commonwealth Bank. "For some industries, like financial services, important new regulations are afoot. Unintended consequences *will* flow from these changes—and there will be few upside outcomes."

Figure 1: Technology and regulation are the biggest external change drivers

In your view, which of the following external drivers of change will have the biggest impact over the next 18 months on your organization?	Total	FS	CIPS	TICE	HC	Gov't
Technological change and IT risks	58%	64%	49%	71%	59%	67%
Increasing regulatory complexity and scrutiny	56%	78%	48%	42%	71%	28%
Changing customer needs/behavior	50%	43%	51%	70%	57%	35%
Government policy changes (fiscal and monetary policy, etc.)	42%	43%	37%	29%	60%	64%
Global economic shifts and uncertainty	42%	41%	49%	41%	15%	33%

Note: FS = financial services; CIPS = consumer and industrial products and services; TICE = technology, information, communications, and entertainment; HC = healthcare; and Gov't = government agencies

Rising concerns about technology-related threats are echoed in PwC's *17th Annual Global CEO Survey*, where 81% of CEOs cite technological advances as the trend that will most transform their business over the next five years. In part, these worries have a basis in sensational cases such as Edward Snowden's leaking of confidential NSA documents and the December 2013 theft of some 110 million Target customers' personal information. But concern also centers on the broader disruptive effects of technological advances in virtually every sector. "There's a significant change coming about as a result of developments in technology," says David Cole, Group CRO at Swiss Re. "It's accelerating the 'time to decay' of any new product or idea. More and more ideas are distributed very rapidly, so replication takes place very rapidly—and not only replication, but improvement."

"There's a significant change coming about as a result of developments in technology. It's accelerating the 'time to decay' of any new product or idea. More and more ideas are distributed very rapidly, so replication takes place very rapidly—and not only replication, but improvement."

—David Cole, Group CRO, Swiss Re

The impact of technology change is particularly acute for TICE companies (71%) and government organizations (67%). In the healthcare and financial services sectors, by contrast, regulatory pressures remain top of mind. "The 'expectation bar' from regulators, investors, and all stakeholders is increasing exponentially" in the financial services sector, says Dr. Toevs at Commonwealth Bank. By contrast, companies in the TICE and CIPS sectors regard changing customer needs/behavior as the key driver (70% and 51%, respectively).

"The common denominator of CIPS and TICE is that both are consumer-sensitive businesses where demand is powerfully affected by technology innovation," says Dean Simone, Leader of PwC's US Risk Assurance practice. "Change is nearly constant in TICE, driven by consumer reception of new and often disruptive technologies, and CIPS has been radically transformed as the consumer and industrial marketplaces increasingly move online." At one technology company, Google, the need to innovate means that there needs to be a focus on controlling upside risks—the threat that the company could miss out on an opportunity if it is not able to deliver as expected, says Google's Chief Audit Executive, Lisa Lee (see "Moving TICE companies up the risk maturity curve," page 27).

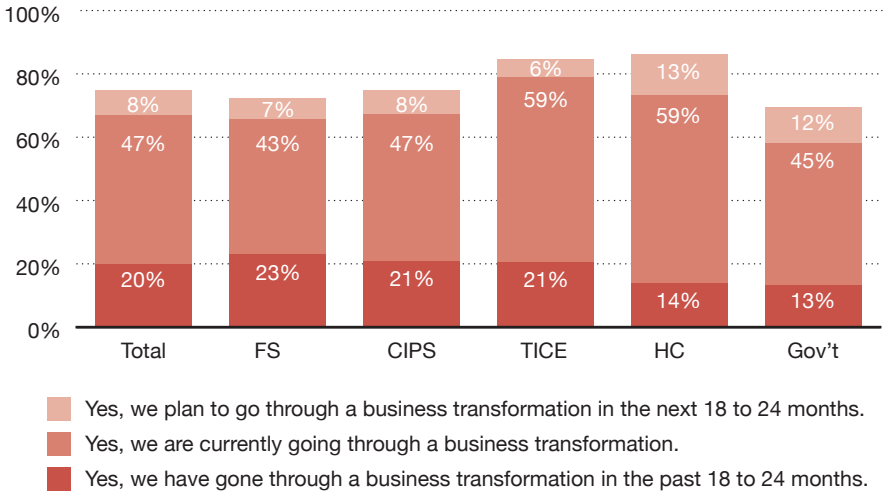
Business transformation has become the norm

In response to these powerful shifts in the market, organizations in all sectors are undertaking dramatic business transformations, altering their strategies and driving radical internal change. In all, some 75% of our survey respondents reported that they are in some stage of transformation (see Figure 2)—a number that's down only slightly from last year (78%), confirming that transformation remains a powerful force.

Indeed, when asked to rank the biggest internal drivers of change over the next 18 months, 71% of survey respondents point to business transformation, including large majorities in all sectors (see Figure 3). Healthcare and TICE, responding to powerful if very different changes in their markets, are more likely than any other sector to be in some stage of business transformation—whether in the midst of a transformation effort, having recently undergone such an effort, or planning such an effort for the next 18 to 24 months (86% healthcare, 85% TICE).

Figure 2: Business transformation sweeps all sectors

Is your organization transforming its business to respond to market shifts?



Note: Excludes "No" and "Don't know" responses

FS = financial services; CIPS = consumer and industrial products and services; TICE = technology, information, communications, and entertainment; HC = healthcare; and Gov't = government agencies

Following business transformation are other, closely related change-drivers: growing reliance on technology and IT systems (59%), innovation around products, services, and business models (52%), and changes in talent, staffing, and resources (38%). For TICE, business model innovation is an especially important driver (66%), while for government, growing reliance on technology is a major concern (66%).

The impact of transformation is important because of its capacity to create cascading risk effects across many business activities—including mergers, acquisitions, and divestitures, cited by almost one third of respondents as a high-impact change. At Eastman Chemical Company, for example, the acquisition of specialty chemicals maker Solutia has compelled executives to ask some fundamental questions about their company's risk management processes and structure. "Probably in the last two years, the biggest focus is our acquisition of Solutia—a $4.8 billion acquisition," says Peter Roueche, Director, Enterprise Risk and Insurance. "Does it give us a different profile of risk? Are there risk processes in place to mitigate these? Are there risks that we didn't identify in due diligence, that we need to address now?"

Figure 3: Business transformation is the dominant internal change driver

In your view, which of the following internal drivers of change will have the biggest impact over the next 18 months on your organization?	Total	FS	CIPS	TICE	HC	Gov't
Business transformation / change management initiatives	71%	70%	49%	67%	77%	78%
Growing reliance on technology and IT systems	59%	63%	54%	55%	58%	66%
Innovation around products, services, and business models	52%	57%	51%	66%	53%	44%
Changes in talent, staffing, and resources	38%	37%	37%	30%	36%	53%
Mergers, acquisitions, and divestitures	32%	28%	39%	41%	43%	6%

Note: Includes top five responses

FS = financial services; CIPS = consumer and industrial products and services; TICE = technology, information, communications, and entertainment; HC = healthcare; and Gov't = government agencies

Spotlight on government

The public sector, which has been buffeted by many of the same economic forces as private companies since the financial crisis, also faces many of the same challenges in managing risk—in some cases to a more severe degree.

For example, public-sector respondents are considerably more worried than overall survey respondents about changes in talent, staffing, and resources (53% vs. 38%). This reflects the difficulty budget-constrained agencies face in recruitment, as well as restructuring and reductions in staffing via attrition. They are also more concerned about a lack of IT skills needed to support new digital strategies (46% vs. 34%). Perhaps as a result, public-sector respondents also are dramatically more concerned that major IT programs will not produce desired results (68% vs. 53% of the overall survey sample).

The public sector is responding to these challenges with determination. In nearly every area of change—from adopting vision statements, risk appetite statements, and enterprise-wide risk rating systems to building the capabilities of the risk function and creating a risk-aware culture across the organization—governmental agencies are as likely as overall survey respondents to prioritize building their capacities.

External shifts + internal change = capability gaps and heightened risk exposure

The combination of external shifts and internal change has heightened risk exposure, opening up capability gaps that traditional risk management systems were not built to address, and that can severely weaken risk management strategies.

"A number of issues come from transformation," says Mark Newlands, Head of Risk Management and Business Assurance at Anglo American. "You can take your eye off what is happening in the markets you operate in if you are too internally focused, and the internal control environment can weaken as people, systems, and processes change."

Indeed, the top three gaps identified in our survey (see Figure 4) relate to the effects of fast-moving internal change: fragmented risk data and analysis (26%), gaps arising directly from business transformation initiatives (24%), and cyber-security gaps (23%).

At a time of intensifying risk, rationalizing data and analytic reports is especially urgent. "At a low level of capability, companies have data in silos, rely on manual processing, and generate static reports—often using simple spreadsheets," says John Sabatini, PwC Principal, Advanced Risk & Compliance Analytics Services. "But companies frequently miss issues that data could have pointed them to, and which have ultimately been the cause of heightened risk or even fines and sanctions."

Again, capability gaps vary by sector: Financial services organizations are notably more concerned with gaps arising due to regulatory complexity (23% vs. 17% of respondents overall). CIPS companies, on the other hand, are more concerned with risks arising from the need to enter developing markets (22% vs. 17% overall).

The results suggest, however, that executives may not fully understand some key capability gaps. In one increasingly crucial area—interconnected risks—relatively few (16%) report significant capability gaps. Yet this is a vulnerability that will require closer attention. "Risk interconnectivity is an area that companies must focus on more, given the dynamic nature of the business and its impact on the risk profile," says Brian Schwartz, PwC US Governance Risk and Compliance Leader, Risk Assurance Services. "This interconnectivity is about understanding how one risk can trigger another."

"You can take your eye off what is happening in the markets you operate in if you are too internally focused, and the internal control environment can weaken as people, systems, and processes change."

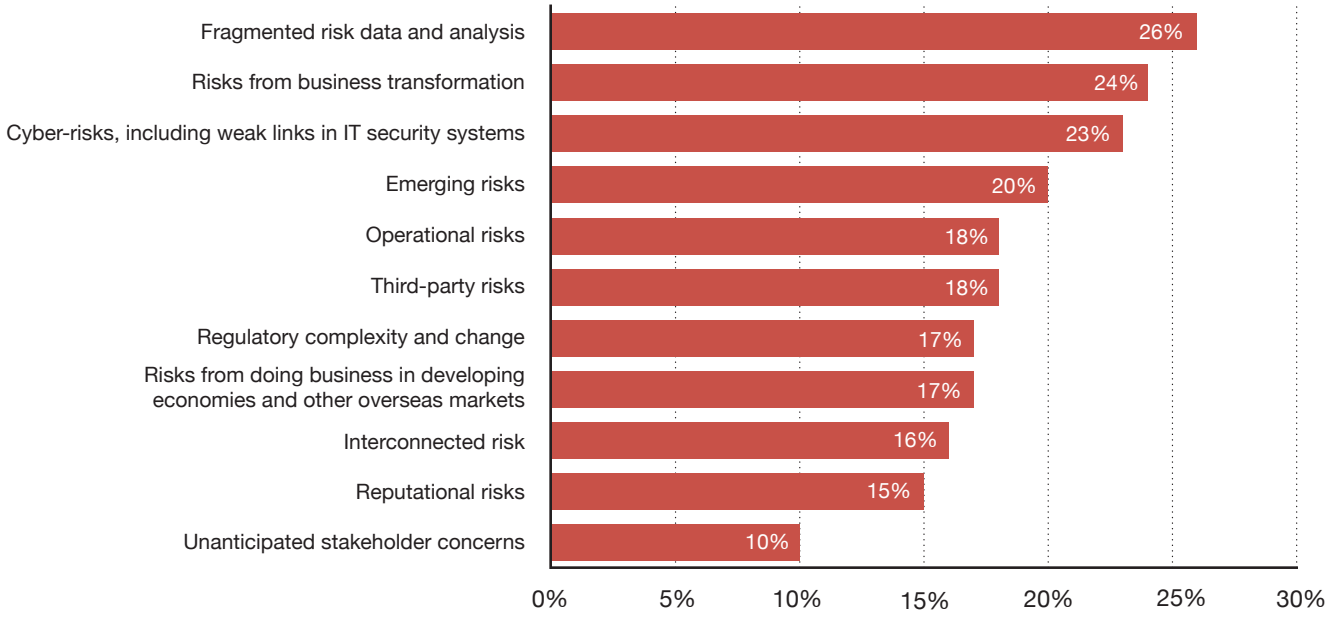
—Mark Newlands, Head of Risk Management and Business Assurance, Anglo American

"IT risks become fatal if the business is not involved. The business and IT need to work in tandem."

—Pat Roche, Vice President, Information Technology Solutions, C. R. Bard

Figure 4: The largest capability gaps involve technology and business transformation

Which areas of risk represent the largest capability gaps for your company today?



Note: Combines "Very significant gap exists" and "significant gap exists" responses

Digital transformation is critical, but executives struggle with implementation

Broadly speaking, the biggest capability gap centers on increasingly technology-dependent business models. Failure of new IT systems to deliver expected benefits ranks as the top technological risk, cited by 53% of respondents (see Figure 5) and ranking as a top-three risk across all sectors. Also of high concern are more frequent and sophisticated cyber-attacks, cited by almost half of survey respondents overall (47%), with financial services and TICE showing notably greater concern (57% and 54%, respectively). News of cyber-attacks spreads more quickly, too, often via social media, and often with reputation-damaging results.

"The potential for successful cyber-attacks is increasing, and social media increases the speed of reporting," says Commonwealth Bank's Alden Toevs. "Incidents are more quickly reported, often with inaccurate estimates of impacts." The risk is especially great for TICE companies, for which customer data is a pivotal asset.

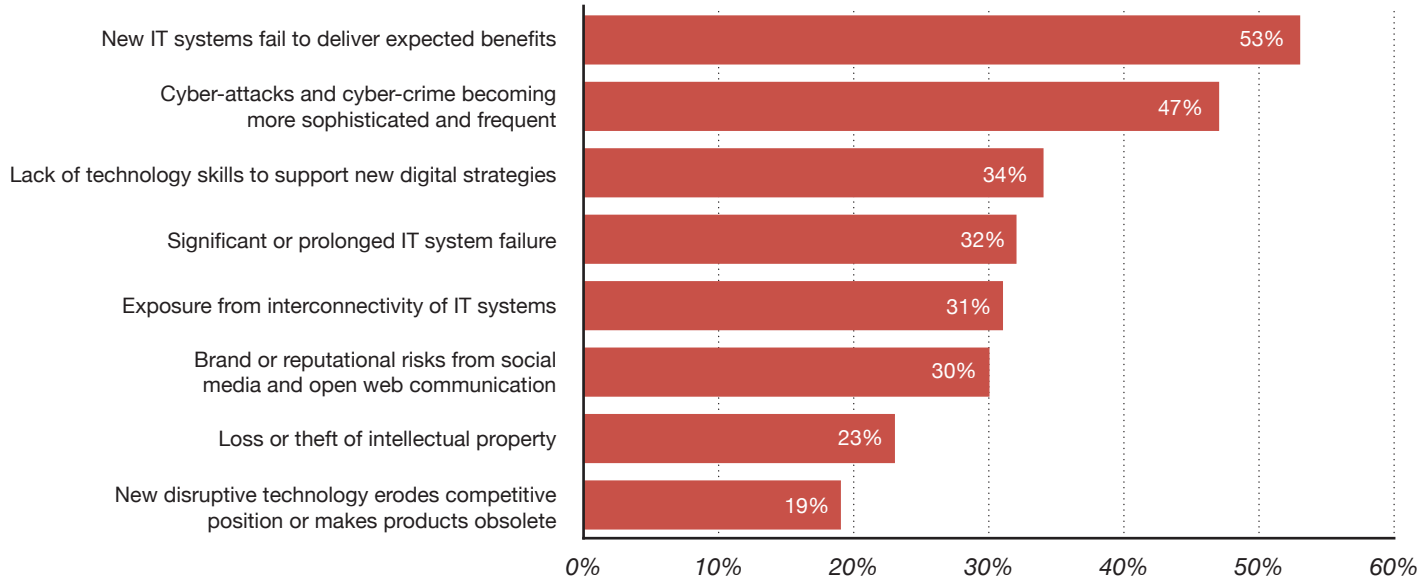
Such threats become more complex and difficult to solve when risk, IT, and the business units are not in frequent communication. "IT risks become fatal if the business is not involved," says Pat Roche, Vice President, Information Technology Solutions, at C. R. Bard. "The business and IT need to work in tandem."

Successful execution of technology projects and strategies requires the tools to implement them and the skills to support implementation. Yet lack of technology skills emerged as a top-three technology risk, cited by at least 30% of survey respondents in every sector. "Data and access to accurate data are becoming more and more important to understanding both clinical and business trends," says Mr. Roche. "It's changing so fast that in order to be competitive, you have to be innovative and take advantage of technology to support the business so you can make better business decisions."

That said, some executives suggest tech risk is something they may never fully master. "We know our systems have been attacked," says Mr. Newlands of Anglo American. "We also recognize it's not possible to eliminate these attacks. What you can do is monitor, and introduce sensible measures to protect yourself." This includes internal as well as external threats: "Managing information internally is just as important as protecting your hardware and software from external threats," he says.

Figure 5: Technological change puts organizations at risk

To what extent do you feel that your organization is at risk from each of the following factors over the next 18 months?



Note: "High risk" responses

Facing a volatile risk environment, companies are scrambling to maintain risk competencies

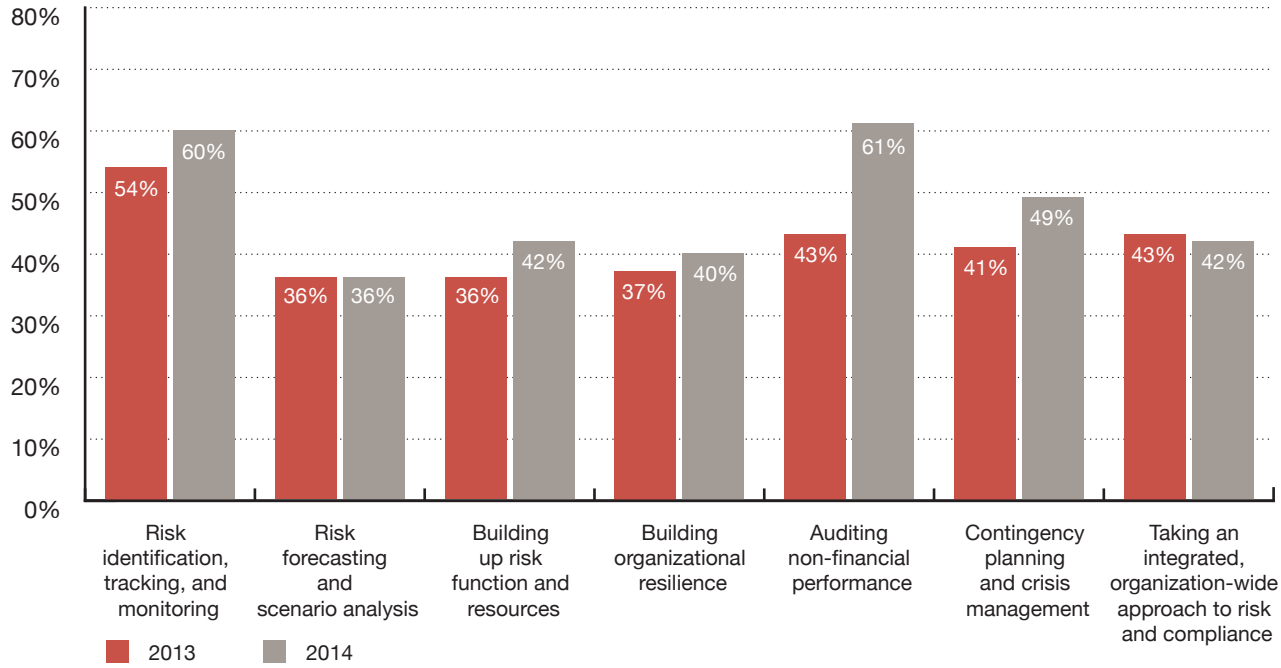
In the face of capability gaps and technology challenges, executives feel they are making progress at maintaining and building their risk management competencies. Compared with last year, larger percentages of respondents are more satisfied with their level of competency in almost all risk management processes (see Figure 6). Nevertheless, some important areas still need improvement: Respondents are least satisfied with their abilities around risk forecasting and scenario analysis, and with competencies involving structure and processes—building organizational resilience, building up the risk function and resources, and taking an integrated, corporate-wide approach to risk and compliance.

Across sectors, financial services companies are most satisfied with their competencies, perhaps owing to more widespread benchmarking against peers. "In our case, learning from others doesn't just mean learning from other insurance companies," says Swiss Re's David Cole. "It means learning from oil and gas companies, learning from pharmaceutical companies, and learning from IT companies."

Executives are least satisfied with their abilities around risk forecasting and scenario analysis, and with competencies involving structure and processes.

Figure 6: Satisfaction levels are growing for most areas of risk competency

How satisfied are you with your organization's current level of competency in each area?



Note: Combines "Somewhat satisfied" and "Very satisfied" responses

Case study: Managing technology change at Eastman Chemical

Disruptive technology—the threat that another company comes up with a better or cheaper version of a key product—is the greatest technology risk facing Eastman Chemical Company, says Peter Roueche, Director, Enterprise Risk and Insurance. "We need to make sure we continue to innovate," he says, "and that we are the ones displacing, not the ones being displaced."

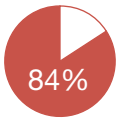
Eastman Chemical addresses this risk through its Innovation Council, staffed by its business vice presidents, general managers, and technology VPs. The council has a different focus than do similar groups at other companies, however: Instead of looking inward, applying an Eastman-specific standard for what is "innovative," it looks outward, at what the market is demanding. And instead of monitoring competitors' research and development, which Eastman believes would be difficult and also unproductive, the council seeks to identify unmet customer needs in the wider marketplace. "What we are looking for are the characteristics our customer wants that some other technology might deliver, and thereby displace our product," says Mr. Roueche.

The Innovation Council's job is to identify and drive development of breakthrough technologies that could either enhance product characteristics that are crucial to customers, or deliver them at a lower price point. As an example, Mr. Roueche cites Tritan™ copolyester, a durable, high-end plastic developed by Eastman that competes with other materials like acrylic and polycarbonate. While it shares many of the same characteristics as those materials, Tritan does not contain Bisphenol A (BPA), a synthetic that the FDA identified in 2010 as potentially hazardous to infants. "We had all these other characteristics that we thought were the selling points, but simultaneously with that, the marketplace was looking for BPA-free replacements. So our product was very successful," says Mr. Roueche.

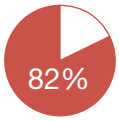
Creating a risk-aware culture to address capability gaps and non-traditional risks

While improving competencies is an important step in closing capability gaps, organizations are making broader changes across three areas: (1) people and culture, (2) strategy and vision, and particularly (3) processes, systems, and technology. The objective is to embed risk awareness across the organization, improve processes to monitor risk, and increase companies' attention to non-traditional risks.

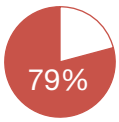
The top-ranking changes that survey respondents have made or plan to make in the next 18 months (see Figure 7) are:



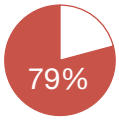
Creating a risk-aware culture (84%), making risk management a priority for people at all levels of the organization.



Developing processes to continuously identify and monitor risks (82%), including non-traditional risks.



Conducting more non-financial audits (79%) to ensure that emerging threats like cyber-security are being addressed.



Integrating risk and business strategies (79%), ensuring that risk is factored into all strategic decisions.

Additionally, 61% have a formal risk management function with dedicated resources distinct from the compliance function, while of those that do not, 20% expect to have one within the next 18 months.

At many companies, the momentum for change appears to be coming from the board. Across numerous categories, board members were far more likely than respondents overall to say their company had made or was planning to make changes, including integrating risk and business strategies (88% vs. 79%), building organizational resilience (81% vs. 68%), and offering effective risk-adjusted incentives (44% vs. 33%).

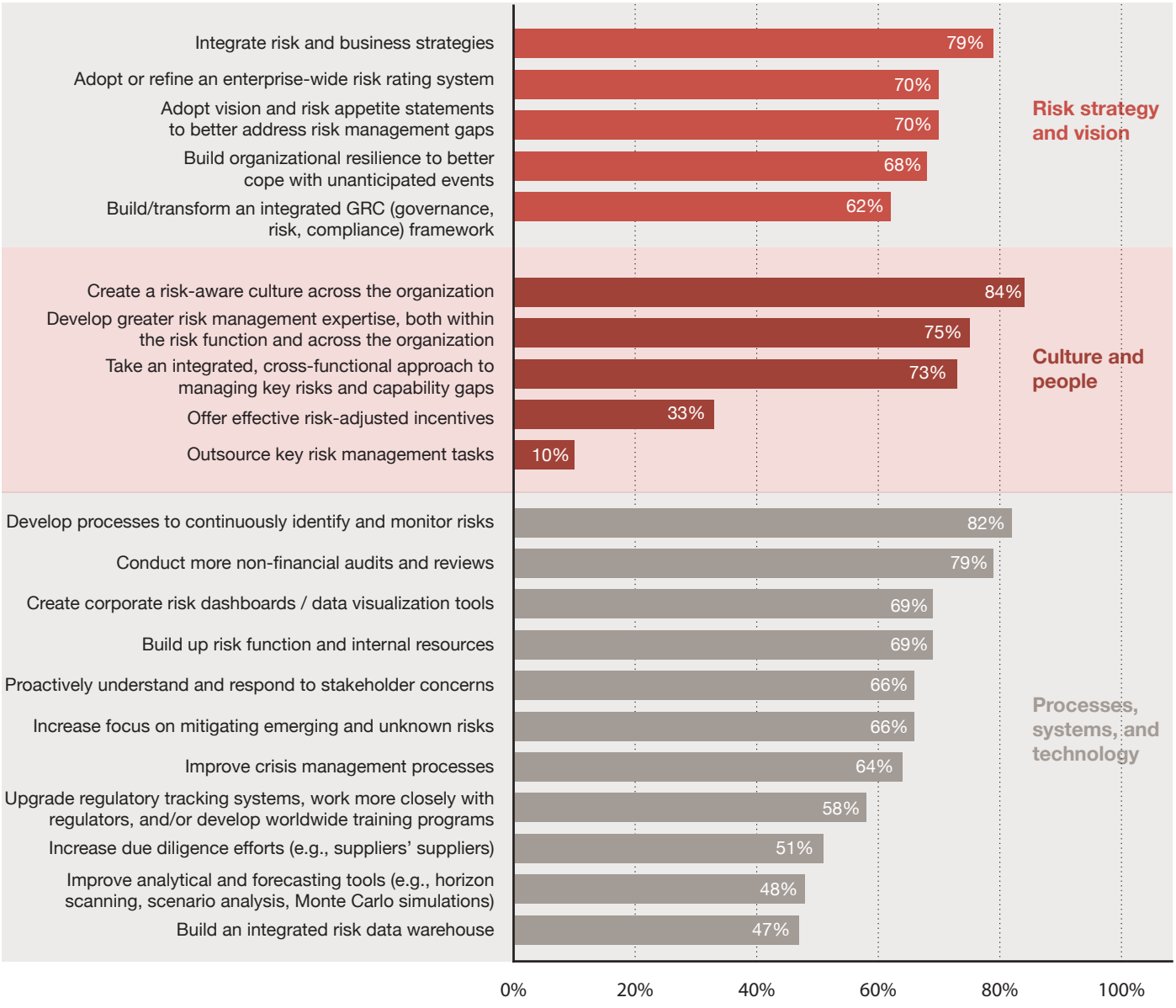
Among the sectors, financial services companies are most likely to be implementing changes in most categories, although the public sector leads in such categories as integrating risk and business strategies, developing processes to continuously identify and monitor risks, and improving crisis management processes.

Several categories reveal a split between small and very large organizations and their medium-sized and large counterparts. Organizations at the smallest and largest ends of the spectrum, facing distinct sets of challenges, are making greater progress at adopting risk appetite statements, building organizational resilience, building up risk function resources, and operating an integrated risk data warehouse. This may reflect the tendency of a company's institutional development to lag behind its growth, but it may also reflect the scale of the challenges. For instance, it can be easier for a small company to integrate risk data using a fairly simple solution (52% say they do so) than for a larger, more complex company (43%).

For many organizations in fast-growing economies, too, improving risk management is part of catching up with global corporate best practices. Comparing responses from organizations headquartered in developing markets and organizations headquartered in industrialized economies, our survey found that those in emerging markets are substantially more likely to be upgrading regulatory tracking systems (73% vs. 54%), adopting risk-adjusted performance incentives (43% vs. 30%), increasing their focus on emerging and unknown risks (79% vs. 64%), and even developing risk data warehouses (65% vs. 42%). Only 52% of North American organizations have adopted a formal risk function, compared with more than 70% in other regions, including the developing world.

Figure 7: Organizations address capability gaps

Which changes have you already made or are you planning to make over the next 18 months to address key capability gaps?



Note: Combines "Already made change" and "Planning to make change over next 18 months" responses

Miscommunication between the management/board level and risk/compliance exacerbates capability gaps

While executives move to close the capability gaps they've identified, they may be missing a key issue: miscommunication between the management/board level and the risk/compliance functions. Our survey revealed a surprisingly sharp disconnect, with top management and the risk and compliance functions disagreeing not only on the type and degree of key risks facing the company, but also about the organization's capabilities. For example, management is less inclined to see risks increasing (68%) than are the risk and compliance functions (80%).

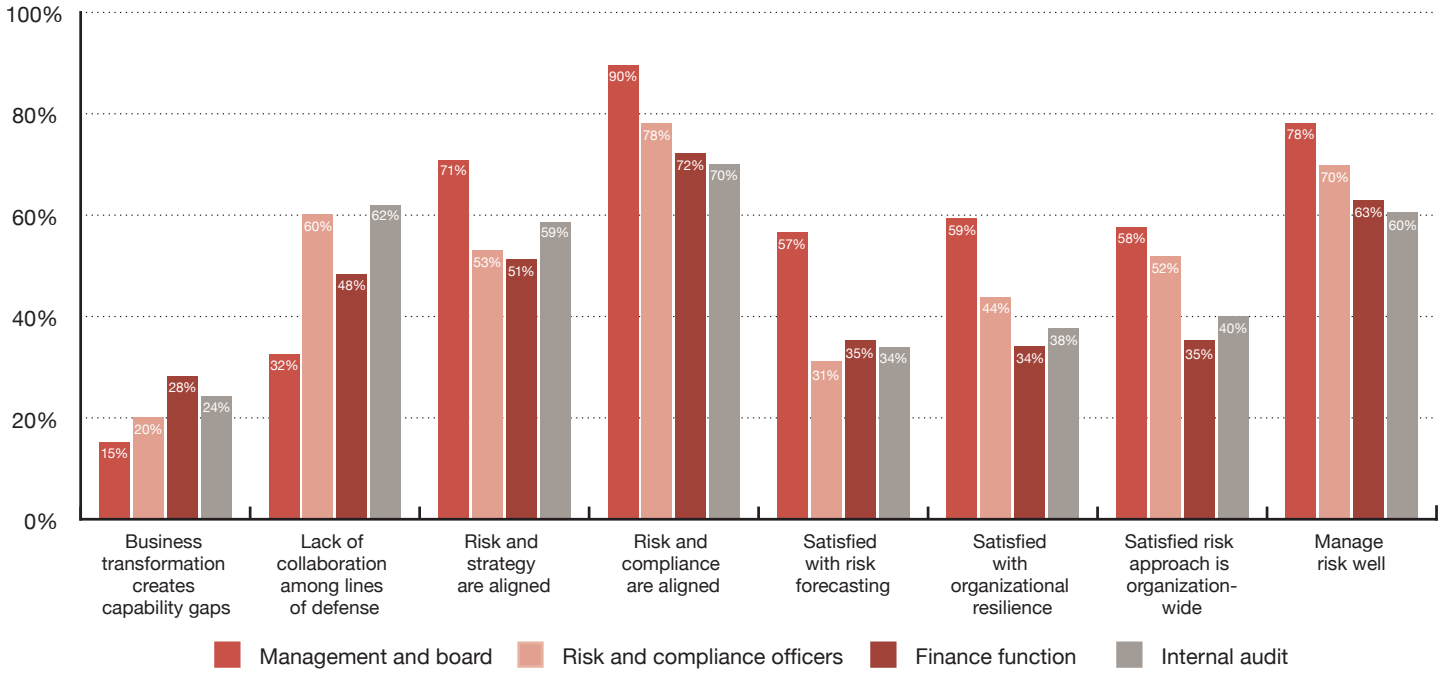
Management's views of some areas of external change also differ from views expressed by risk/compliance: Management devotes more attention to strategic issues such as global economic shifts and uncertainty (41% vs. 32%), while risk and compliance concentrate on day-to-day risks such as the velocity of change in the business environment (41% vs. 30%).

This disconnect extends to perceptions of the company's competence. While 60% of risk/compliance officers say lack of internal collaboration exposes them to capability gaps, only 32% of management agrees (see Figure 8). This disagreement suggests that management lacks a strong grasp of the day-to-day challenges with which the risk/compliance functions must contend, and that stronger collaboration between the two is needed.

Part of the solution may be to place more timely analysis in the hands of management, says Scott Greenfield, PwC US IT & Project Assurance Leader, Risk Assurance Services. For instance, he says, "In a bank, business systems are constantly being updated. Hence, it is not enough to keep your risk system updated: The link between your risk system and, for example, your trading system, must also be updated." If not, management may receive faulty information on risk exposures—even though the reports they are viewing show no sign of trouble.

Management devotes more attention to strategic issues such as global economic shifts and uncertainty, while risk and compliance direct their attention to day-to-day risks such as the velocity of change in the business environment.

Figure 8: Management/board and the risk functions hold differing views of risk



Note:

Business transformation creates capability gaps: Which areas of risk represent the largest capability gaps for your company today? (Risks from business transformation)

Lack of collaboration among lines of defense: Do you believe that lack of collaboration among your company's lines of defense could be exposing your company to capability gaps in your defense against risk?

Risk and strategy are aligned: Is your company's risk management function aligned with other business functions today? If not, do you anticipate that it will be in the next 18 months? (Strategic planning)

Risk and compliance are aligned: Is your company's risk management function aligned with other business functions today? If not, do you anticipate that it will be in the next 18 months? (Compliance)

Satisfied with risk forecasting: How satisfied are you with your organization's current level of competency in each area? (Risk forecasting and scenario analysis)

Satisfied with organizational resilience: How satisfied are you with your organization's current level of competency in each area? (Building organizational resilience)

Satisfied risk approach is organization-wide: How satisfied are you with your organization's current level of competency in each area? (Taking an integrated, corporate-wide approach to risk and compliance)

Manage risk well: Overall, how well do you think your organization manages risk?

Despite improvements, collaboration among the lines of defense still requires optimization

Organizations report considerable success in aligning risk functions with other areas to strengthen risk culture and strategy. Concerns remain, however, that collaboration among the three lines of defense (business units, risk and compliance, and internal audit) in identifying, monitoring, and effectively managing critical risks is still not deep enough to protect the organization from capability gaps.

Such collaboration shares equal importance with robust risk management competencies and strong collaboration between top management and risk management.

Respondents agree that close collaboration between risk-related functions is vital to ensure a shared view of business risk up, down, and across the enterprise: 93%, for example, say internal audit's core responsibilities include focusing on critical risks and issues the company faces, and 77% say that these responsibilities include providing insights on emerging risks and how the company is addressing them.

Happily, respondents also report a great deal of progress in fostering broader alignment of the risk functions with other parts of the organization, and predict further progress to come. Alignment is close to ubiquitous today between risk management and functions traditionally considered its partners—internal audit (80%), finance (76%), and compliance (72%)—and most organizations also report alignment with other key areas, including operations, IT, legal, and human resources. For all of these, alignment is expected to top 80% in 18 months (see Figure 9). The exception is sales and marketing, where less than half of organizations report alignment with the risk functions today, although nearly three out of four expect to achieve it over the next 18 months.

This increased focus on aligning sales and marketing with the organization's risk functions may reflect rising concern over risk emanating from social networks and other digital channels generally managed by marketing. AutoNation, for example, recently added a department head of marketing to its risk committee. "This VP has responsibility for e-commerce," says the company's Senior Director of Risk Management, Dennis Royer. "So this is giving us insight into all of the new areas of cyber-risk."

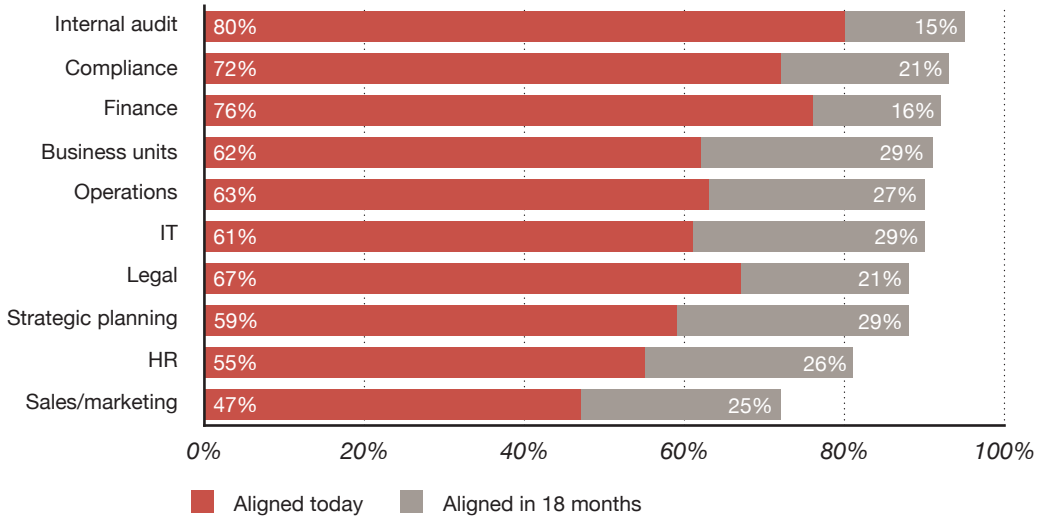
Despite the progress organizations have made at aligning risk/compliance and the other lines of defense, executives believe that alignment is not yet sufficiently pervasive. Almost 60% of survey respondents overall still express concern that lack of collaboration among the three lines of defense could be exposing their company to capability gaps.

"Companies without a fully integrated view of risk across the three lines of defense are not positioned to optimize risk management efforts for efficiency," says Jason Pett, PwC US Internal Audit Services Leader, Risk Assurance Services. "Also, and even more importantly, without a collective view, you'll fail to eliminate holes in risk management by assuming that risks are covered by other parts of your risk infrastructure, when they are not, or are not fully covered."

Despite the progress organizations have made in fostering collaboration between the business units, risk and compliance, and internal audit, executives believe that alignment is not yet sufficiently pervasive to prevent exposures due to capability gaps.

Figure 9: Risk functions are aligned with more parts of the organization

Is your company's risk management function aligned with other business functions today? If not, do you anticipate that it will be in the next 18 months?



Case study: Anglo American takes risk culture to the mine site

In the mining industry, safety is a primary concern. Yet in recent years, competitive pressures and the need to control costs have assumed a larger profile, forcing companies to rebalance their risk priorities. At industry giant Anglo American, "We are looking to restructure, remove costs, and remove duplication and waste where we can. But at the same time, we must operate safely and improve our safety record—if we don't get that right, it can have an impact on our license to operate a mine," says Mark Newlands, Head of Risk Management and Business Assurance.

The new initiatives mean greater responsibilities for the managers of Anglo American's individual mines. "We embarked upon some very significant projects, probably later in the cycle than competitors, so the delivery of those projects becomes critical," says Mr. Newlands. Managers at the work site will therefore have to broaden their remit beyond safety risks and put particular emphasis on successfully managing operational risks.

While risk or audit might seem the logical place to locate operational risk responsibility, this creates the danger that site managers will see any operational risk tools as primarily oriented toward reporting. To avoid this misperception, the company is creating a more formal risk process for managers who previously were mainly concerned with safety. "We need to make sure risk is really understood at the operational level and that the management team at the mines sees risk management as a tool that can help them deliver their production targets," says Mr. Newlands.

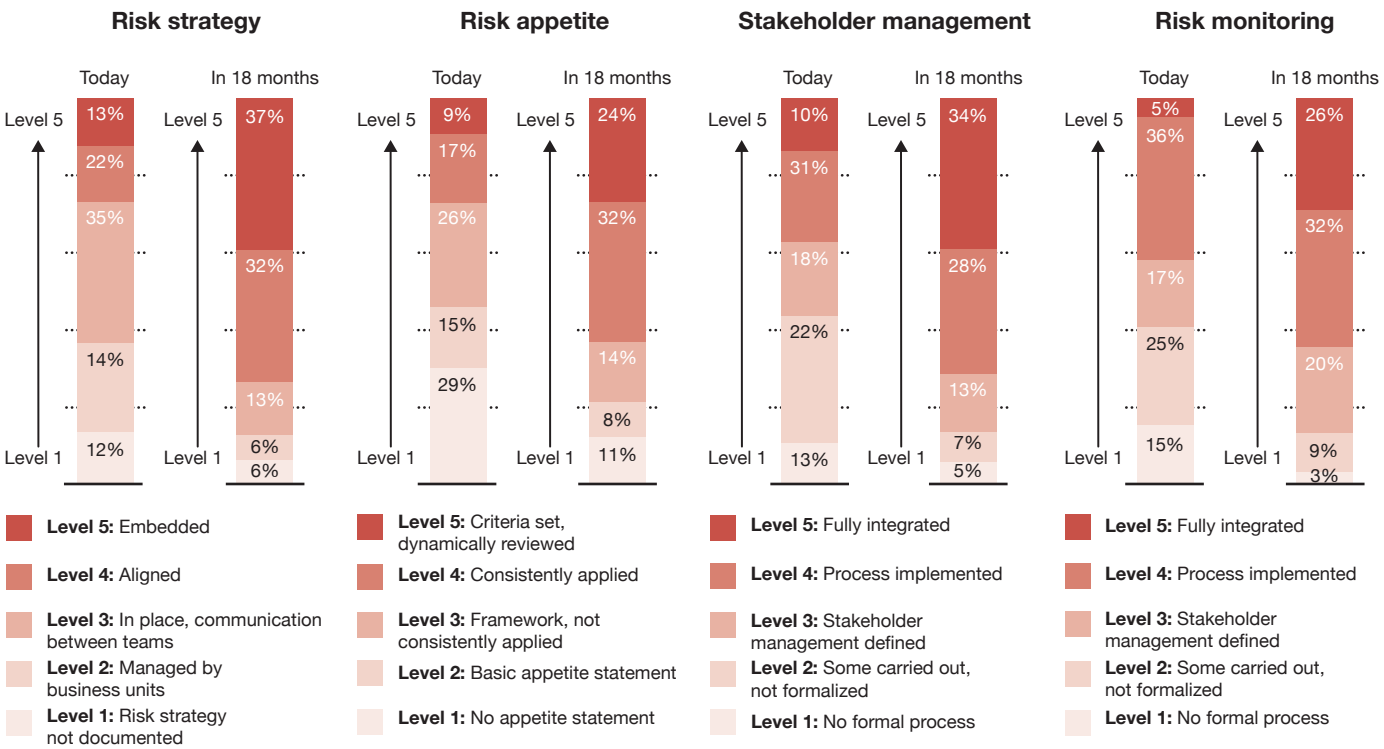
This is, in the first instance, a cultural change. It entails managers defining what risks they are exposed to and what they need to do to mitigate those risks—and it entails bringing these questions to the front of their minds. "It's not just a question of saying to the managers, 'Okay, you are now responsible for assessing risks—off you go,'" says Mr. Newlands. "There needs to be some structure behind it, there needs to be some training provided, and there need to be tools and ongoing guidance for the initial period, including some systems implementation."

Moving up the maturity curve is an imperative

Understanding that addressing capability gaps needs to be part of a more holistic approach, organizations are moving toward higher levels of maturity in all six areas of risk management they rated in this study (see "Survey and interview methodology," page 5). Four categories, however—risk management strategy, risk appetite, stakeholder management, and risk monitoring and reporting—stand out with a more dramatic expected pace of change than is predicted in the other two areas (risk culture and risk-adjusted performance incentives). Majorities or near majorities across all sectors—and large majorities of top management, board members, and risk/compliance officers—expect to be at levels 4–5 (denoting the most highly developed risk capabilities) within 18 months (see Figure 10). The finance function, however, is much less optimistic about the rate of progress across almost all areas of maturity.

Figure 10: Majorities approach maturity in four key risk categories

In these categories, majorities or near majorities across all sectors expect to be at levels 4–5 (most mature) within 18 months.



Note: Excludes "Don't know" responses

Getting to these levels means prioritizing specific sets of goals, as detailed below.

Risk management strategy. Prioritizing risk management strategy means aligning business and risk strategy and embedding risk strategy across core business processes over the next 18 months. Dennis Royer describes how AutoNation is achieving this alignment: "The risk review committee meets quarterly, selects certain risks that have surfaced, and does a 'deep dive' with the owner, putting mitigation efforts in place and then searching as a team for new ways to further reduce that risk." While financial services leads in the prediction of maturity, with more than 80% of sector respondents expecting to reach levels 4–5 in the next 18 months, large majorities in other sectors expect to do so as well (see Figure 11).

Risk appetite. Reaching levels 4–5 means defining risk appetite, applying it consistently, and using the risk appetite statement to drive strategy and business decisions. More than half of respondents in all sectors except government expect to be at levels 4–5 in 18 months.

Stakeholder management. Risk maturity in stakeholder management means establishing processes to communicate effectively with stakeholders. Much effort in this area concentrates on social media. Alden Toevs at Commonwealth Bank says that in addition to having a full-time social media team, his bank has "new social media training and awareness initiatives for our people, to raise understanding of social media and cyber-risks."

Figure 11: Strong progress expected at building risk maturity across four areas

Industry progress indicators in areas of strong progress (current)	FS	CIPS	TICE	HC	Gov't
Risk management strategy	50%	29%	29%	32%	29%
Risk appetite	41%	20%	18%	20%	22%
Stakeholder management	53%	36%	38%	37%	40%
Risk monitoring and reporting	56%	35%	36%	33%	38%

Industry progress indicators in areas of strong progress (in 18 months)	FS	CIPS	TICE	HC	Gov't
Risk management strategy	83%	65%	62%	65%	64%
Risk appetite	73%	51%	51%	56%	43%
Stakeholder management	72%	59%	62%	56%	50%
Risk monitoring and reporting	73%	52%	56%	53%	51%

Note: Which stage of maturity best describes current elements of your risk management framework, and the one you hope to have in place over the next 18 months? (Proportion at levels 4–5)

FS = financial services; CIPS = consumer and industrial products and services; TICE = technology, information, communications, and entertainment; HC = healthcare; and Gov't = government agencies

Risk monitoring. Maturity in risk monitoring includes monitoring, aggregating, and reporting risk activities, and integrating that reporting with day-to-day management tools. Although the majority of total respondents expect to move to levels 4–5 within 18 months, the picture is different when broken down by sector. While financial services respondents show a clear trend toward levels 4–5 maturity, most respondents in CIPS, healthcare, and government will still be at levels 3–4 in 18 months.

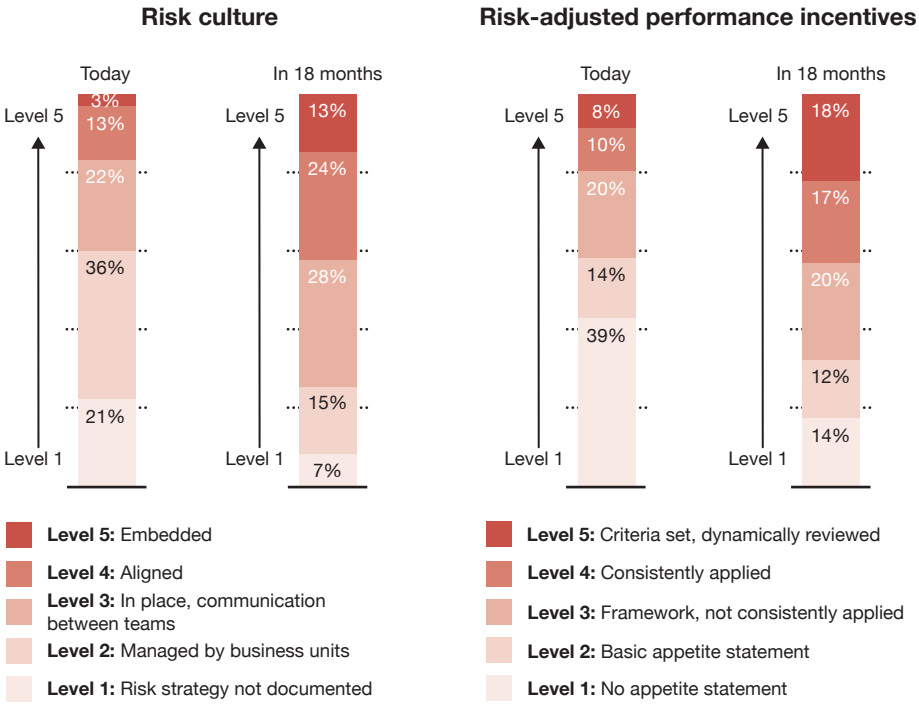
A major aspect of risk monitoring is data analytics, because of the opportunity it presents not only to understand risks better but to respond more quickly. "Companies must leverage data analytics and technology-enabled forecasting, monitoring, and aggregation techniques throughout the risk lifecycle, to inform their risk view and then monitor it along the way," says PwC's Jason Pett. "Companies that effectively leverage data analytics are able to see risks moving in near-real time, and position the organization for a prompt and appropriately intense response."

In financial services, which enjoys wide leads in risk maturity across all six categories today and expects to build on them over the next 18 months, this technology-enabled approach to risk maturity is increasingly common. At Commonwealth Bank, for instance, recent updates include upgrading the operational risk system and integrating it globally. This provides real-time reporting, thus enabling greater transparency for risks, controls, control assurance testing, incident management, issues management, and key risk indicators. "Other notable recent improvements are a multi-year finance and risk data warehouse program and improvements in our liquidity risk measurement systems," says Group CRO Alden Toevs.

The undiscovered country: Boosting risk culture and defining risk-adjusted performance incentives

Despite the clear advances organizations are making in most elements of risk management maturity, many companies, varying by sector, still show critical capability gaps in the areas of risk culture and risk-adjusted performance incentives.

Figure 12: Less progress expected in risk culture and performance incentives



Note: Excludes "Don't know" responses

"As well as a full-time social media team, we have new social media training and awareness initiatives for our people to raise understanding of social media and cyber-risks."

—Alden Toevs, Group CRO, Commonwealth Bank of Australia

Risk culture. Over half of organizations in almost all sectors expect to be at levels 3–4 in 18 months, which means expanding risk culture analysis more fully across the organization and developing process benchmarking around risk culture. Only 13%, however, will have taken the additional steps of instituting ongoing benchmarking of risk processes and adopting automated tools to assess the effectiveness of risk culture training. Even in financial services, which leads all sectors in attention to risk culture maturity, less than half of all sector respondents (47%) and barely more than half of management and board members (54%) expect their company to reach levels 4–5 in 18 months. While 84% of survey respondents say they have created a risk-aware culture across the organization or expect to do so, these maturity predictions suggest that organizations may not be putting all the necessary elements in place to assure achievement of higher risk culture maturity.

Risk-adjusted performance incentives. When asked about their organizations' anticipated future performance in terms of defining the linkage between business incentives and risk strategy, and integrating those with strategic and tactical plans at all organizational levels, less than half of management and board members—and only 41% of risk and compliance officers—said they expect to reach levels 4–5 in the next 18 months. Only in financial services do more than half of organizations expect to be at those levels, while one third of TICE companies and government agencies expect to still be at levels 1–2. Yet progress here is crucial to maintaining organizations' long-term sustainability, says Jason Pett: "Incentives driven by financial metrics alone run the risk of driving behavior that maximizes short-term financial success while ignoring the longer-term view of enterprise health and sustained success."

Figure 13: Few sectors expect substantial progress in 18 months

Industry progress indicators in areas where gaps may persist (current)					
	FS	CIPS	TICE	HC	Gov't
Risk culture	24%	14%	11%	13%	15%
Risk-adjusted performance incentives	33%	14%	9%	10%	7%

Industry progress indicators in areas where gaps may persist (in 18 months)					
	FS	CIPS	TICE	HC	Gov't
Risk culture	47%	33%	35%	34%	39%
Risk-adjusted performance incentives	53%	29%	25%	29%	22%

Note: Which stage of maturity best describes current elements of your risk management framework, and the one you hope to have in place over the next 18 months? (Proportion at levels 4–5)

FS = financial services; CIPS = consumer and industrial products and services; TICE = technology, information, communications, and entertainment; HC = healthcare; and Gov't = government agencies

Risk leaders are moving aggressively to improve risk processes and systems

Our survey revealed a connection between organizations' success at moving up the risk maturity curve and the extent to which they are upgrading and leveraging risk tools and systems. Risk leaders are 59% more likely than others to be improving analytical tools, building an integrated risk data warehouse (52%), and/or upgrading regulatory and tracking systems (44%). Risk leaders are also more likely to be making improvements in areas that receive less attention among overall respondents—for example, they're twice as likely to have adopted or be planning to adopt risk-adjusted performance incentives.

"Becoming a risk leader is not just about process, although that's critical," says PwC's Brian Schwartz. "It also involves creating a risk-aware culture. What these data analytic tools have in common is they make risk monitoring and reporting easier and more accessible. Risk-based incentives ensure that risk management is part of managers' everyday thinking throughout the organization. Both help create that risk-aware culture."

These efforts are producing results, judging from respondents' level of satisfaction with key aspects of their risk processes and structures (see sidebar, "What are the benefits of risk leadership?" page 26).

Risk leaders are more likely than early-stage companies to:

- Say they manage risk well (97% for risk leaders vs. only 36% for early stage)
- Have a formal risk function (85% vs. 43%)
- Align the risk function with challenging areas such as strategic planning (85% vs. 29%), IT (87% vs. 28%), HR (81% vs. 25%), and sales/marketing (79% vs. 19%)
- Say they are somewhat or very satisfied with their organization's current levels of risk competency, including risk identification, tracking, and monitoring (91% vs. 35%), risk forecasting and scenario analysis (82% vs. 13%), building up organizational resilience (85% vs. 13%), and building up the risk function and resources (85% vs. 15%)

Risk leaders are also substantially less likely to report significant capability gaps—relating, for example, to business transformation (11% vs. 32% of early-stage companies), fragmented risk data and analysis (12% vs. 42%), reputation risk (9% vs. 19%), and interconnected risk (9% vs. 25%).

Leading companies we interviewed have also made significant progress in many of the following areas:

- **Continuously identifying and monitoring risks.** AutoNation maintains a risk inventory, which it updates continually and presents to the board once a year.
- **Non-financial audits and reviews.** Commonwealth Bank has devoted more attention to non-financial risks. Specific projects have centered on health and safety, environment, talent, and brand/reputation risks.
- **Integrated risk data capabilities.** AutoNation is continuing to increase its data capabilities, including segmenting its information to a more granular level—a capability it believes it must have to stay competitive.
- **Cyber-security**. C. R. Bard recently created a steering committee that includes members from the business units, IT, HR, and legal, to address the potential risks of digital and social media.
- **Risk-adjusted performance incentives.** Commonwealth Bank's remuneration framework stipulates that all individual incentive outcomes are reviewed and may be reduced or clawed back in light of any risk management issues.

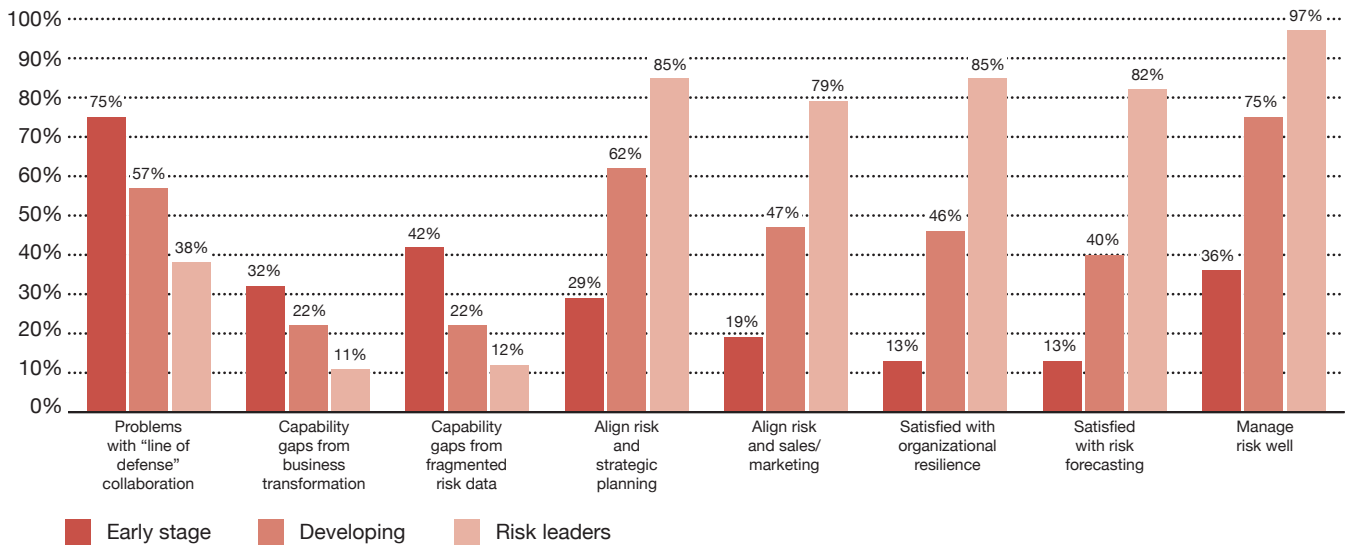
Our survey revealed a connection between organizations' success at moving up the risk maturity curve and the extent to which they are upgrading and leveraging risk tools and systems.

What are the benefits of risk leadership?

Risk leaders differ considerably from other organizations, both in the degree of difficulty they experience with collaboration and capability gaps and in their level of satisfaction with aspects of risk management itself. They are far more likely to align the risk functions with other parts of the organization, they report fewer problems fostering collaboration between lines of defense, and they're less likely to suffer capability gaps from business transformation or fragmented risk data.

Two thirds of early-stage companies, by contrast, report problems with collaboration across the three lines of defense. They also are overwhelmingly unsatisfied with their competency at risk forecasting and building organizational resilience.

Figure 14: Differing outcomes for risk leaders vs. early-stage and developing companies



Note:
Problems with "line of defense" collaboration: Do you believe that lack of collaboration among your company's lines of defense could be exposing your company to capability gaps in your defense against risk?
Capability gaps from business transformation: Which areas of risk represent the largest capability gaps for your company today? (Risks from business transformation)
Capability gaps from fragmented risk data: Which areas of risk represent the largest capability gaps for your company today? (Fragmented risk data and analysis)
Align risk and strategic planning: Is your company's risk management function aligned with other business functions today?
Align risk and sales/marketing: Is your company's risk management function aligned with other business functions today?
Satisfied with organizational resilience: How satisfied are you with your organization's current level of competency in each area? (Building organizational resilience)
Satisfied with risk forecasting: How satisfied are you with your organization's current level of competency in each area? (Risk forecasting and scenario analysis)
Manage risk well: Overall, how well do you think your organization manages risk?

Moving TICE companies up the risk maturity curve

Risk management at companies in the technology, information, communications, and entertainment (TICE) space reflects the fact that many of these firms are relatively new and operate in fast-growing, volatile, fiercely competitive businesses. TICE companies are more likely to be undergoing or planning to undergo business transformation than any sector except healthcare. They express much greater concern about risks related to business volatility, increased competition, and cyber-security than they do about risks stemming from regulation or internal processes.

Troublingly, these companies are also less likely to be making changes to improve their risk processes and culture, such as building an integrated GRC framework, developing greater risk management expertise across the organization, building an integrated risk data warehouse, or offering risk-adjusted performance incentives.

Yet the pace of change in their businesses, and the resulting internal and external pressures, pose particularly acute challenges for TICE companies. New technologies transform competitive dynamics every few years; business models must in turn be reinvented. Rather than simply protecting their existing processes, one of the key risks for TICE companies that are engaged in a constant cycle of innovation and new product launches is the threat that an unforeseen obstacle could derail or spoil the timing of a new offering. "With risk management, the picture is changing every day," says Melvin Flowers, Corporate Vice President of Internal Audit at Microsoft. "You have both the environment changing and the business objectives changing, and understanding the impact of both of these things is the secret sauce of risk management today."

To meet these challenges, TICE companies need to establish a high degree of coordination and communication across business units and multiple lines of defense—something few have achieved thus far. An exception is Microsoft, which is undertaking an initiative to transform and centralize the risk function. As part of "One Microsoft," a realignment launched last year to focus the company on a single strategy and make the organization more collaborative, the company has shifted its risk personnel from product teams to a central team that includes corporate-wide ERM and internal audit. While the risk personnel remain physically located in the businesses they serve, uniting them organizationally is expected to make risk management more efficient overall.

"Centralization of the risk function together with internal audit and ERM was crucial," says Mr. Flowers. "In evaluating risks, we are now able to work with management one time instead of two to three times, and audit can leverage the deeper risk assessments produced by ERM." Microsoft will move away from annual risk assessments by internal audit in favor of rolling assessments across the company, enabling it to detect and address critical risks in real time, he says.

As part of this initiative, Microsoft also has put a high priority on better communication and a common understanding of risk between management and the risk function. To aid in this task, "we are beginning to get our cross-company risk vocabulary and definitions tightened up," says Mr. Flowers. "It was the move toward centralization of the risk function that made that possible." The objective is in part to make sure that a conversation is taking place around risk throughout the company, he says. Since a risk in one area "can affect someone downstream, we have to make sure through this conversation that everyone recognizes and accepts this and knows the consequences."

What this means for your business

Risk imperatives for 2014

The aim of risk management is twofold: sustainability—making sure the odds favor the company's survival—and the ability to capitalize on change. This means continuing to look forward and becoming ever more sensitive to the complex interplay of risk and opportunity.

Swiss Re's David Cole gives an example of how his company addresses this imperative: "We have designated groups and individuals with a mandate to help us look ahead," he says. "Not just to come up with a five-year financial plan, but to know what is going on out there that is going to affect our business, and to agree how we want to respond—sometimes at a very granular level. It's to ensure the longevity of Swiss Re by making sure we stay aware of changes in the social, political, and economic environments."

This cannot be a piecemeal process. Continuing business transformation, and the capability gaps created by heightened external and internal change, make it urgent that organizations improve their risk management maturity. Happily, our survey and one-on-one interviews reveal that most organizations are working to do so, addressing the distinct set of imperatives that apply at each stage as they move up the maturity ladder.

Early-stage organizations. These companies need to ensure that the right resources are focused on risk management, and begin the process of de-siloing their risk processes by extending them across the organization. These organizations should:

- Produce a formal risk strategy document and implement it at the business unit level.
- Roll out a formal stakeholder management / communications process to monitor and manage the company's relationship with employees, investors, regulators, community activists, and other internal and external stakeholders.
- Develop an internal audit function that provides support in building the risk and compliance infrastructure.
- Transform risk monitoring from an ad hoc activity to a regular process, starting at the board level.
- Develop a formal risk culture analysis and perform it regularly.
- Create risk-adjusted performance incentives, starting at the board and senior management level.

Developing organizations. Companies that have passed the early stage can start to develop more robust risk assessments, monitoring, and auditing around hot areas including technology risk (especially cyber-security issues), regulatory risk, and business transformation. Companies in the CIPS and TICE sectors should implement customer needs monitoring as well. Developing organizations should:

- Align risk and business strategy documents.
- Apply their risk appetite statement beyond business units, to the entire organization.
- Continually assess and measure the alignment of risk management posture and activities across the three lines of defense.
- Initiate regular monitoring of risk activities and aggregation of data and analysis at the business unit level.

"We have designated groups and individuals with a mandate to help us look ahead—not just to come up with a five-year financial plan, but to know what is going on out there that is going to affect our business, and to agree how we want to respond."

—David Cole, Dutch and American Group CRO, Swiss Re

- Make risk monitoring results and in-depth analysis part of regular reports to senior management.
- Expand risk culture analysis organization-wide, and benchmark the process regularly.
- Link business incentives and risk strategy and apply across the organization.

Risk leaders. Maintaining leadership in risk management means regularly reviewing, evaluating, and updating the company's processes, incentives, and risk culture. Risk leaders should:

- Embed risk strategy across the organization, and regularly review and update that strategy.
- Apply the risk appetite statement to all business decisions across all business and functional units, dynamically reviewing and updating risk appetite criteria.
- Update and assess the effectiveness of their integrated stakeholder management / communications strategy.
- Regularly test and upgrade the risk monitoring and reporting system.
- Continuously measure the effectiveness of risk culture training tools.
- Review and update risk-adjusted performance incentives to make sure they remain integrated with strategic and tactical plans at all levels of the organization.

Even for risk leaders, the journey to higher levels of capability never ends. As our survey results show, risk leaders are far more likely than other organizations to be planning further risk capability improvements. "You can't stay stagnant when it comes to your risk approach," says Pat Roche at C. R. Bard. "You need to change with the times and evolve to take advantage of what technology can do to support the business and mitigate risk."

"You need to change with the times and evolve to take advantage of what technology can do to support the business and mitigate risk."

—Pat Roche, VP, Information Technology Solutions, C. R. Bard

www.pwc.com

To have a deeper discussion about this subject, please contact:

Dean Simone, Partner
US Risk Assurance Leader
dean.c.simone@us.pwc.com
267 330 2070

Jason Pett, Partner
US Internal Audit Leader
jason.pett@us.pwc.com
410 659 3380

Brian Brown, Principal
Risk Assurance Innovation Leader
brian.brown@us.pwc.com
949 241 5052

John Sabatini, Principal
Advanced Risk & Compliance Analytics Leader
john.a.sabatini@us.pwc.com
646 471 0335

Brian Schwartz, Principal
US Risk Assurance—Performance GRC Leader
brian.schwartz@us.pwc.com
202 729 1627

Christopher Michaelson, Director
PwC's Global Advisory Strategy and Risk Institute
christopher.michaelson@us.pwc.com
612 596 4497

Ron Kinghorn, Principal
US Advisory—Governance, Risk, and Compliance Leader
ron.kinghorn@us.pwc.com
617 530 5938

Neelam Sharma, Director
US Risk Assurance Strategy, Sales, and Marketing Leader
neelam.sharma@us.pwc.com
973 236 4963

PM-14-0271 SL